Exhibit 40

Excerpts of Steven Colquitt
Deposition Transcripts

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

SECURITIES AND EXCHANGE COMMISSION,
Plaintiff,
vs.
SOLARWINDS CORP. and TIMOTHY G. BROWN,
Defendants.
Case No. 23-cv-9518-PAE

VIDEOTAPED DEPOSITION OF
STEVEN COLQUITT
Austin, Texas
Wednesday, September 18, 2024

Reported by:
Micheal A. Johnson, RDR, CRR
Job No. 240918MJ

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

SECURITIES AND EXCHANGE COMMISSION,
Plaintiff,
vs.
SOLARWINDS CORP. and TIMOTHY G. BROWN,
Defendants.
Case No. 23-cv-9518-PAE

Videotaped Deposition of STEVEN COLQUITT, taken on behalf of Plaintiff, at Latham & Watkins, LLP, 300 Colorado Street, Suite 2400, Austin, Texas, beginning at 9:26 a.m. and ending at 4:56 p.m. on September 18, 2024, before Micheal A. Johnson, a Registered Diplomate Reporter, Certified Realtime Reporter, and Notary Public of the State of Texas.

APPEARANCES:
ON BEHALF OF PLAINTIFF:
U.S. SECURITIES AND EXCHANGE COMMISSION
BY: Christopher J. Carney
John J. Todor
100 F Street, NE
Washington, D.C. 20549
(202) 256-7941
carneyc@sec.gov
todorj@sec.gov

ON BEHALF OF DEFENDANTS
SOLAR WINDS CORP. AND TIMOTHY G. BROWN:

LATHAM & WATKINS LLP
BY: Serrin Turner
Nicolas Luongo
1271 Avenue of the Americas
New York, New York 10020
(212) 906-1330
serrin.turner@lw.com
nicolas.luongo@lw.com

ALSO PRESENT:

Becky Melton
Laurie Hakes
Jason Bliss

VIDEOGRAPHER:
Timothy Desadier

INDEX
STEVEN COLQUITT
September 18, 2024

DEPOSITION EXHIBITS
STEVEN COLQUITT
September 18, 2024

EXHIBIT NO.	DESCRIPTION	MARKED
Exhibit 1	Amazon Article, What is SDLC (Software Development Lifecycle)?	24
Exhibit 2	Slide Presentation SW-SEC00007881 - SW-SEC00007892	33
Exhibit 3	Slide Presentation, SolarWinds Secure Development Lifecycle SW-SEC00150762 - SW-SEC00150799	44
Exhibit 4	January 30, 2018 E-mail, Steven Colquitt to Brno Engineering Management, et al. SW-SEC00238141 - SW-SEC00238142	90
Exhibit 5	January 30, 2018 E-mail, Timothy Brown to Steven Colquitt SW-SEC00336293 - SW-SEC00336294	122
Exhibit 6	September 20, 2018 E-mail, Rani Johnson to Joe Mitchen SW-SEC00237608 - SW-SEC00237609	132
Exhibit 7	May 1, 2018 E-mail, Joe Kim to IT Department, et al. SW-SEC00016513 - SW-SEC00016521	147

DEPOSITION EXHIBITS
STEVEN COLQUITT
September 18, 2024

EXHIBIT NO.	DESCRIPTION	MARKED
Exhibit 8	June 19, 2018 E-mail, Steven Colquitt to Eric Quitugua and Jamie Hynds SW-SEC00048985 - SW-SEC00048987	160
Exhibit 9	SolarWinds KBT Offsite, DOIT and R&D SW-SEC00262250 - SW-SEC00262261	165
Exhibit 10	July 2019 MSP Products Security Evaluation SW-SEC00166790 - SW-SEC00166799	168
Exhibit 11	March 9, 2018 E-mail, Timothy Brown to Jonathan Lozinski SW-SEC00013553 - SW-SEC00023558	172
Exhibit 12	October 22, 2018 E-mail, Matej Uhrin to Steven Colquitt, et al. SW-SEC00023343 - SW-SEC00023344	175
Exhibit 13	January 30, 2018 E-mail, Lukas Vrbecky to Steven Colquitt SW-SEC-SDNY_00055079 - SW-SEC-SDNY_00055080	197

Austin, Texas, Wednesday, September 18, 2024
9:26 a.m. - 4:56 p.m.

PROCEEDINGS

THE VIDEOGRAPHER: This is the videotaped deposition of Steven Colquitt in the matter of the Securities and Exchange Commission versus SolarWinds Corp. et al., Case No. 23-cv-9518-PAE. This deposition is being held at Latham & Watkins at 300 Colorado Street, Austin, Texas.

Today's date is September 18th, 2024. Time on the video is 9:26 a.m. My name is Timothy Desadier, certified legal video specialist with Gradillas Court Reporters located at 400 North Brand Boulevard, Suite 950, Glendale, California 91203.

Would counsel and all present please voice identify themselves.

MR. CARNEY: Christopher Carney for the Securities and Exchange Commission.

MR. TODOR: John Todor, Securities and Exchange Commission.

MR. TURNER: Serrin Turner, Latham & Watkins, for defendants.

MR. LUONGO: Nicolas Luongo, Latham &

Watkins, for defendants.

MS. MELTON: Becky Melton, SolarWinds.

MR. BLISS: Jason Bliss, SolarWinds.

THE WITNESS: Steven Colquitt, SolarWinds.

THE VIDEOGRAPHER: And we have one in the Zoom.

MS. HAKES: Laurie Hakes, Analysis Group.

THE WITNESS: Would the court reporter please swear in the deponent.

STEVEN COLQUITT,
having been first duly sworn, was examined and testified as follows:

EXAMINATION

BY MR. CARNEY:

Q. Good morning, Mr. Colquitt.

A. Morning, Chris.

Q. We just met off the record. As I said, my name is Chris Carney. Could you state and spell your full name for the record.

A. My name is Steven Colquitt, S-t-e-v-e-n, C-o-l-q-u-i-t-t.

Q. And, Mr. Colquitt, have you ever had your

A. Not in the sense of delivering product to customers, no.
Q. And did you have responsibility in a different sense?
A. Yes.
Q. And what was that responsibility?
A. It began with -- at some point in 2016, 2017 as we were preparing to be ready for GDPR compliance in May of 2018, there were some changes again within the company where I was given responsibility to represent engineering and preparing for GDPR readiness, and that's when I became more involved with the Orion product suite.
Q. And GDPR is the general data protection regulation?
A. Yeah, I believe that's the acronym. Yes.
Q. And that's a European standard; is that right?
A. Yes.
Q. And you said you were given the responsibility to represent engineering in preparing for GDPR readiness.
What responsibilities were you given?
A. I was liaisoning between the engineering leadership that was in place at the time that had

the responsibilities for delivering Orion to customers between those team members and the consultant, the GDPR readiness consultant, that was representing SolarWinds.
Q. And who was that consultant?
A. I don't recall. Or I should say I don't remember.
Q. That's fair enough. And what sort of -- when you were doing this liaisoning between engineering leadership and the consultant, what were your specific responsibilities?
A. I don't remember specifics. This was six-plus years ago. I do know at the time he would ask for certain artifacts and then I would try to produce those artifacts by either looking into our documentation platform or communicating with the existing leadership at the time, who would then point me to our documentation platform most of the times.
Q. And when you say "artifacts," what do you mean?
A. I mean documentation.
Q. And what would that documentation document?
A. Our engineering processes and activities.

Q. And were those the engineering processes and activities for software development?
A. Among -- anything that engineering was doing to produce customer-facing software was documented in some -- some form.
Q. And in terms of the GDPR requirements, were there additional requirements that you understood had to be met to develop software?
A. I don't recall anything that we weren't already doing. It was more of an effort to produce a consistent and concise set of documentation around those activities.
Q. And are you familiar with the concept of a secure development lifecycle?
A. It depends in which context you're using that phrase.
Q. What are the different contexts that you've heard that phrase used?
A. When I use the phrase "secure development," especially when I use it in the sense of not a title, so if I just refer to secure development, it's just referencing the indication that there are security activities that are a part of your development lifecycle.
When you use the phrase as a title, it

could potentially mean something different. In my case it would refer to a process that would overlay those particular security activities.
Q. So let me try to break apart those two different contexts. You said the first context is that it could be part of your development lifecycle; is that right?
A. What could be?
Q. So that a secure development lifecycle you said could be part of your development lifecycle; is that right?
A. So generally when you refer to software development, it is a lifecycle. You go through a set of processes that have to be completed before you can deliver that software. Security is a part of that lifecycle. So when I refer to, lower case, a secure development lifecycle, I'm indicating that along with all the other activities there are also security activities that happen as part of that lifecycle.
Q. Okay. Great. Actually -- and is a -- and is that -- the overall process, is that referred to as a software development lifecycle?
MR. TURNER: Objection to form.
A. When you refer to the overall process,

Q. And -- but other parts of the requirements are the performance of the product, right?
A. Yes.
Q. And you mentioned a little while ago that you can talk about secure development lifecycle in the context of the overall development of software, right?
A. Yes.
Q. And then the other context is you can talk about secure development lifecycle as a stand-alone thing; is that right?
MR. TURNER: I'm going to object to form.
A. I'm not following.
BY MR. CARNEY:
Q. So you described two contexts. So we just talked about the secure development lifecycle as part of the overall software development lifecycle. What was the other context that you said that you can talk about secure development lifecycle?
A. In the beginning I referred to a distinction between secure development lifecycle and a process entitled Secure Development Lifecycle. Is

that what you're asking me to do -- to explain that?
Q. Yes.
A. As I mentioned earlier, when you refer to a secure development lifecycle as just a phrasing, not a title, you're indicating that as part of your development lifecycle you're also focused on security. One way to better provide visibility and consistency is to enhance the processes in which you may overlay what is titled a Secure Development Lifecycle.
Q. Okay. And so now I want to focus on what is titled a Secure Development Lifecycle. What is that?
A. It is a set of processes that overlay the existing security activities and help bring those into a set of documentation or processes that can be tracked and communicated more efficiently.
Q. So when you say it's a set of processes that overlay the existing security activities, what do you mean by that?
A. In the context of SolarWinds, we were performing multiple aspects of security activities in our development process. Overlaying a process added better visibility into a very large organization's activities and made it easier to

report on and track those activities.
Q. And can you explain what you mean by "overlaying a process"?
A. It means surfacing from a -- to make visible in a large organization where you have many teams, many roles of differing seniority levels and involvement, ensuring that everybody has a visibility into those security activities.
Q. And how do you go about doing that?
A. There are probably many aspects, many ways to address that. One such way would be to add additional documentation at the end of the release that consolidates the outputs of all those activities into a single document.
Q. You said one such way. Are there other ways of creating a process?
A. I mean, I'm not a process -- I'm not a program manager. I'm sure -- I'm making an assumption that there's probably hundreds of ways you can improve process. I focused on a few specific things that would improve process at SolarWinds.
Q. And what were the few specific things that you focused on?
A. So one was the addition of what is

referred to as a final security review. So rather than having each team independently do their reviews and sign off, it was bringing them all together for a complete view of the posture, just to improve the visibility of what the teams have been doing from their testing and design.
Q. And you had mentioned a few things. Were there other things besides that, the FSR?
A. Yes. Some of the -- we have -- we follow what's called a release checklist. Those are milestones at each phase. They included some security milestones and we expanded those milestones to bring a few more visibility points to the release checklist.
Q. Are there any particular milestones that you can think of that you added?
A. Without referencing a checklist right now, I can't remember at the time what was added. It would have been a focus on planning -- security activities during planning and design which we were doing and just making sure there was a sign-off on that. The final security review was added. I don't recall what the other ones are at the moment.
Q. Okay. And so besides the final security review and the updated checklist, are there other

Q. So in the design phase, how do you assess risks?
A. As teams receive a requirement to implement a piece of code, those teams are assessing risks at that time as they're designing. And it's differing levels. It may be a simple solution, it may be a complex solution where architecture may be involved.
Q. You said it may be a complex solution where architecture may be involved. What do you mean by that?
A. If data is crossing multiple trust boundaries, it may be a complex solution that require a -- what's called a feature spec where engineering and architecture will collaborate to design the correct implementation.
Q. And what kind of tools are teams using to assess risk as they're designing?
MR. TURNER: Objection just to the vague form of the question.
A. To design software tools use IDEs provided by, for example, Microsoft provides an IDE that we use. Those IDEs are used to design that software, and then documentation. Confluence is our platform for documenting or writing documents.

BY MR. CARNEY:
Q. What is IDE?
A. It's an acronym for something development environment. I'm totally forgetting the "I" at the moment. Integrated development environment.
Q. So in the design phase are they analyzing the code to assess risks?
MR. TURNER: Objection to the form of the question.
A. During the design phase we will analyze a requirement that we've gotten from product management and flesh out the implementation from that requirement.
BY MR. CARNEY:
Q. And you also mentioned that you do risk assessment in the implementation phase. Is that a different type of assessment than in the design phase?
A. It's pretty simple in that as an engineer if I am receiving a requirement to take user input and store it in a database, I am making an assessment that there is a risk. At that point at which the data leaves the user and goes to the database, then I will implement a security control. It can be as simple as a conversation between two

engineers, it can be as complex as a design document. It depends on the situation.
Q. So when you say "implement a security control," what's an example of a security control?
A. Implementing authorization controls to make sure you have the right access to be able to access that data. A password, certificate-based authentication, validating user input, encrypting data, those type things.
Q. And I think you touched on this earlier, but just to clarify, we talked a bit earlier when I showed you the Exhibit 1, the Amazon document, there's the planning phase, the design phase, the implementation phase, the testing phase and the deployment phase.
Is security being considered in all those phases?
MR. TURNER: Just objection. Are we talking about at SolarWinds or are we talking about at Amazon? What?
MR. CARNEY: At SolarWinds.
A. Can you rephrase the question?
BY MR. CARNEY:
Q. Sure. And I'm really just trying to clarify that I had used the design phase as an

example, but in all phases of software development, security is being assessed; is that fair?
A. Where applicable security is assessed at every single phase of development. Yeah.
Q. Okay, great. Thank you.
(Deposition Exhibit 3 marked for identification.)
BY MR. CARNEY:
Q. Mr. Colquitt, once again, you take as much time as you need to look over the document as you're answering the questions.
For the record, Exhibit 3 is a PowerPoint presentation entitled Secure Development Lifecycle, Steven Colquitt, and it begins at Bates stamp SW-SEC00150762.
Are you familiar with this document?
A. Yes, I am.
Q. Did you prepare this presentation?
A. Yes, I did.
Q. And do you recall when you prepared it?
A. Leading up to December of 2017 I would have worked to produce this.
Q. And what was the purpose of this document?
A. I was introducing a new process to

overlay our security activities that we were labeling Secure Development Lifecycle, capital S, capital D, capital L. That was the title. So I was producing materials to help present that to engineering.

Q. And when you say that "overlay our security activities," what do you mean?

A. It means that during the time of GDPR readiness, as I talked to engineering, as I searched through all of our documentation, I found a tremendous amount of artifacts pointing to our security testing and practices that we were doing at the time. I found it very difficult to compile that into a single source of documentation and I saw an opportunity to improve our processes to bring more awareness and visibility to those activities. So I produced some marketing materials that were presented at a technical summit in the Czech Republic in December of 2017.

MR. TURNER: Can I just ask a clarifying question? Just in terms of marketing, can you explain what you mean? Do you mean outside marketing?

THE WITNESS: I mean internal marketing. I would be asking engineering to make

some changes to their processes and to do some extra documentation, so I was trying to market this as -- socialize it with them.

MR. TURNER: Thank you. I just didn't want to create a confusion.

MR. CARNEY: Thanks.

BY MR. CARNEY:

Q. And the technical summit in the Czech Republic, was that an internal SolarWinds technical summit?

A. Yes, sir.

Q. And you'll notice on the first page it has some notes underneath the slides. Are those your notes?

A. I have to assume. I don't remember if those are my notes or if those are part of the template that I used. I believe those -- I think those are probably my notes.

Q. And the first note says: High-level SDL training and then in parentheses it says: No operational content.

Do you know what that means, no operational content?

A. I don't know what I meant. I can assume that what I was suggesting is we were using a term

within SolarWinds. I had heard the term "operationalize" used referring to processes in the past. I think I was replicating that here to mean -- I was going to introduce this new process, train teams and then operationalize the new process, meaning implement it. So I think it's just terminology for myself.

Q. Okay. And then the next note says: Bar, and then in parentheses it says: What we want to achieve over 2018.

Do you know what you meant by that?

A. Again, I think I'm referring to improving the process that's being documented here as the SDL.

Q. And then the next sentence says: We will be audited.

Do you know what you meant by that?

A. I suspect that the initial -- or I suspect that that's referring to GDPR, which was the initial reason I was pulling all these documentation artifacts together.

Q. And, sir, if I could ask you to turn to the third page, the page ending in 764 with the Agenda.

Do you see that?

A. Yes, sir.

Q. And the first agenda item is: What is an SDL? Let me ask you, at this point when you were doing your presentation, was the concept of an SDL something that was new to SolarWinds?

A. I don't know if the general concept was new to SolarWinds in engineering. From -- this process would have been new to SolarWinds.

Q. And just for the record, when you say "this process," what are you referring to?

A. What I'm stating is that we were already following the tenets of a secure development lifecycle, lower case. We were already participating in security during design. We were testing, we were doing vulnerability, penetration testing, we were assessing the results of those tests and we were determining based on the results of those tests the security posture of our product.

All those things were already happening. So when I refer to the SDL here, I'm referring to the process that overlays and exposes those activities in a more -- a broader perspective to all of engineering and others who might be consuming the results of that -- those activities.

Q. Sir, if I could ask you to turn to the page ending in 766 and it says: What is a secure

Q. But I'm just asking here in this context, it's describing a security training; is that fair?
A. It says security training.
Q. And so is security training focused on secure design and coding?
A. It can be -- it can be. It can be focused on what the current security posture within the industry is seeing. It can be focused on different tactics and techniques that malicious actors are using. Very broad.
Q. So it could focus on -- and correct me if I'm wrong, on best practices in secure design and coding?
A. It could take from what are considered best practices, the ones that are applicable for that particular engineering team.
Q. And could it also refer to industry standards for secure design and coding?
A. Again, industry standards is very broad and within a standard across an entire software industry, there's going to be things that are applicable to a particular team and particular software product.
Q. Is security training a requirement of following the SDL at SolarWinds?

MR. TURNER: Objection to form.
A. The SDL overlaying, again, is a process that enables each of these things to happen. It enables security training. Teams were involved in security training as part of the -- part of our software development lifecycle.
BY MR. CARNEY:
Q. So is the SDL a process to be followed?
MR. TURNER: Objection to form.
A. Can you rephrase that?
BY MR. CARNEY:
Q. Sure. Sure. You've described a number of times the SDL as being a process that overlays existing activities. And I guess what I'm wondering, is the intent of setting up this process having a process to follow?
A. So we have --
MR. TURNER: Objection to form.
A. We followed a Agile frame methodology as an approach. Within that, there were processes. We followed a release checklist full of milestones that included security. The SDL was an overlay on top of that that exposed and gave visibility into those activities at a much higher level and centralized and formalized that documentation.

BY MR. CARNEY:
Q. And what was the purpose of centralizing and formalizing the documentation through this SDL process?
A. The catalyst was to consolidate formal documentation for GDPR readiness.
Q. Were you using the SDL process in an effort to track security activities to improve performance?
MR. TURNER: Objection to form.
A. So that was a two-part question. Which question do you want me to answer?
BY MR. CARNEY:
Q. Well, so let me -- I'll break it apart. Were you using the SDL process to track security activities?
A. Security activities were already being tracked. The SDL gave exposure and made it much more easier for us to pull that together. It also enabled us to better communicate to other departments what engineering was doing from a security perspective.
Q. And when you say it made it easier to pull that together, pull what together?
A. So engineering, again, is a very large

organization, a very large code base and multiple teams, each team producing artifacts. At the time those artifacts weren't being produced in one centralized way for us to consume. They were each producing their own artifacts, which made it very difficult to consolidate all that information.
Q. Was the -- and so now my sort of -- in that context, my earlier question, the SDL process that you were standing up, was that a centralized process that you wanted the engineering teams to follow in developing software?
A. I wanted the SDL process to help reinforce what we were already doing as well as add a few additional tracking processes, including the final security review which was one of the biggest changes that would have to be adopted.
Q. And was one of the goals of this process to improve the performance of the security activities?
MR. TURNER: Object to form.
A. There is always a goal to improve in whatever you're doing. I would not say -- the goal of the SDL, again, was to give visibility into what we were already focused on and what we were already doing.

requirements might require security control. And during the secure development phase or during the development phase you will implement that security control, along with all the other feature implementation.

Q. And it looks like subcomponents of that are secure design and secure coding.

What is secure design?

A. It's the next step of assessing a requirement. I need to implement a security control. The design part would be how will I do that. The secure coding part is the actual implementation.

Q. Is threat modeling part of secure development?

A. Threat modeling is inherent. In fact, what we just did was threat modeling.

Q. When you say "what we just did," what do you mean?

A. This exchange that we just had where I explained that when I assess a particular requirement, I identify a risk and I mitigate that risk, that is threat modeling.

Q. And at SolarWinds, who is responsible for conducting threat modeling?

A. Any engineer involved within implementation. He may make that assessment on his own or he may work with architecture to produce a more complex solution to mitigate those risks.

Q. Does SolarWinds use any external consultants or entities to do threat modeling?

A. I'm -- I can't be definitive with that. I don't know what the individual teams may -- or may have done with threat modeling.

Q. But in your experience, the SolarWinds was threat modeling that was done internally by SolarWinds employees?

A. Absolutely.

Q. And just with respect to secure design, does that require that all third-party and open source components that are planned to be used in the design are scanned for vulnerabilities?

A. We use a third-party application to scan and assess our third-party libraries, yeah.

Q. And what is -- what is that third party that you use?

MR. TURNER: Sorry, third-party application?

MR. CARNEY: Sorry, third-party application, yeah.

A. There were multiple tools. One that I recall was called Black Duck. There are other tools we were using internally for doing scans. I gave a list of those tools to -- to the attorneys. I don't recall every name of the tools that we're using.

BY MR. CARNEY:

Q. When you say you gave them a list, when was this?

A. I produced an artifact out of Confluence, that was our documentation store, from our security team that listed all of the tools that we were using to do vulnerability, pen testing and other security assessments.

Q. You might not know this, but was this, the intent to produce to the SEC, the document?

A. I don't know what the intent of where it was to go, but I was just showing that as of -- you know, even prior to 2018 we were already using -- we were already using -- we were following these security practices already and we were using these tools.

Q. So all the tools you just described were ones you were using prior to 2018?

A. Yes.

Q. And were those tools being used on all

SolarWinds products?

A. My responsibility were security and tools portfolio and I was aware of Orion products because of my association with that particular leadership. So I know it was being used there. I can't speak to the rest of the products that I wasn't responsible for.

Q. And I think you touched a little on secure coding already, so forgive me if you already said. But what is the secure coding aspect of this?

A. So, again, once you've made an assessment that there happens to be a potential risk and you've determined a solution to mitigate that risk, it's just phrasing the idea that you're now implementing that piece of code. And these are just broad labels to kind of indicate the phases of development we go through.

Q. And was secure coding in place for all of the SolarWinds products that you were familiar with as of the time you put this presentation together?

A. Yes, it was.

Q. How do you know that?

A. Documentation and because we were following the processes for secure coding.

Q. All right. The next part of the circle

to release, we go through a phase where we do additional testing until we've achieved a particular quality bar, along with a lot of other ancillary supporting activities to prepare to release the product. As part of that we added an additional process there to bring all of the security activities across a double-digit number of teams into one centralized review called a final security review.

Q. And how did that differ from what was being done before?

A. Previously it was just being done individually on each team. So if you wanted to understand the posture, you had to go to each team individually.

Q. Is there an audit as part of the final security review?

MR. TURNER: Objection to form.

A. The final security review is bringing all of the artifacts and results and assessments of our testing together into a central form that's then reviewed by stakeholders.

BY MR. CARNEY:

Q. So is that in itself an audit?

MR. TURNER: Objection to form.

A. You can choose to label it that way.

BY MR. CARNEY:

Q. So is the final security review, is that part of the secure development that is described in the security statement?

A. By label this is an additional process. At the time and related to the security statement, teams were doing their assessments of the results of their development and the results of their testing and determining whether we reached a quality and security bar to support a release.

MR. TURNER: Can I just try a clarifying question if it would help?

MR. CARNEY: Yeah, go ahead. Sure.

MR. TURNER: When the security statement was published in early January 2018, by that point had you implemented a final security review as part of the secure development lifecycle?

THE WITNESS: What were the dates again?

MR. TURNER: Beginning of January 2018.

THE WITNESS: At that point we had updated the -- I can't recall exactly what the date to the day was, but at the beginning of 2018 we had

updated the release checklist with a requirement to have a final security review.

So teams, depending on their release cadence coming into their next release, would have started with the final security review.

BY MR. CARNEY:

Q. Okay. Thanks. I guess what I was trying to understand, you had mentioned earlier that the security training, the requirements analysis, secure development, security testing, those are all requirements of the secure development lifecycle described in the security statement, right?

MR. TURNER: Objection to form.

A. Analyzing what you're going to implement as an engineer is a standard practice. Testing what you've implemented is a standard practice. Reviewing and assessing the outputs of what you've implemented and tested is a standard practice and was all part of the security statement. That was indicated in that document.

BY MR. CARNEY:

Q. Right. I guess what I was trying to understand, was this -- these requirements related to the release that you described here, is that also something that's encompassed in following the secure

development in the security statement?

MR. TURNER: Objection to form, he's already testified he didn't write the security statement. The security statement says what it says. What exactly are you asking him?

MR. CARNEY: So a number of times when I was asking about this secure development lifecycle that's laid out here on this slide, he tied it back to the security statement and said these were all -- when I asked if they were requirements of SolarWinds' secure development lifecycle, he said they're requirements embodied in the security statement. And so I was trying to understand whether that also applied to this category as well. So just trying to --

MR. TURNER: Yeah. Hang on. I just object to the use of the word "requirements" without any further definition of the term.

But go ahead, if you have another question.

A. I'm lost in that question. If you're asking me if we were applying the activities that supported what is listed in the security statement, the answer is yes. It's inherent in software development that you have to understand what is

A. I don't recall the exact number. Five or less.
Q. And you say in the bottom e-mail: I think it's important that our engineering teams be aware of this which is a public-facing security statement on solarwinds.com. Please share with your teams.
And then were you including a link to the SolarWinds public security statement?
A. Based on the text of that link, I believe that's what I was linking to.
Q. And then did you copy and paste the software development lifecycle portion of the security statement into the text of your e-mail?
A. Yes, I did.
Q. And this might seem obvious based on what you've testified to already, but why was it that portion of the security statement that you were pasting into your e-mail?
A. Because the software development lifecycle is directly related to what engineering does.
Q. And is it more directly related to the work that you did than perhaps the other portions of the security statement?

A. I'm -- you can -- I lost you on that question.
Q. Sure. Sure. So the security statement has a number of other areas besides software development lifecycle, right?
A. Are you referring to the complete security document?
Q. Exactly.
A. Now in that context, what's your question?
Q. So my question is then is it fair to say that you were copying the software development lifecycle portion into the text of your e-mail because that's the portion of the security statement that relates the most to the work that you do?
A. An accurate statement would be that I copied that in because the software development lifecycle statement is related to the engineering activities that produce software that we sell to customers.
Q. And why did you think it was important that your engineering teams be aware of it?
A. Exactly for that reason, awareness. If you recall, I gave you an example earlier. When I worked at Altiris as an associate developer, I was a

brand new -- I was very focused, very limited in my seniority. I didn't have visibility. That was something that overall I was working to improve across SolarWinds was to bring more awareness and visibility to all activities, not just security. Just happened to be we were examining this particular one at this time.
Q. Okay. And you see you sent that out on Thursday, January 25th; is that right?
A. Yes.
Q. And then it looks like the top e-mail is five days later, the following Tuesday; is that right?
A. I don't know what day that is. I know it was 5:00 in the afternoon. Almost 5:00.
Q. And it's January 30th --
A. January 30th.
Q. -- 2018?
And you say -- in the first line you say: Managers, I have gotten feedback that we don't do some of the things that are indicated in the statement below.
First of all, the statement below refers to the software development lifecycle section of the SolarWinds security statement; is that right?

A. It is referring to both paragraphs of that complete statement.
Q. Okay. And by "that complete statement," you mean the software development lifecycle?
A. Lifecycle.
Q. And so first of all, who was giving you this feedback?
A. I received this via an e-mail from one engineering manager.
Q. And who was that engineering manager?
A. His name was Lukas Vrbecky, L-u-k-a-s, V-r-b-e-c-k-y.
Q. And sitting here today, how do you recall that you received this feedback from Lukas Vrbecky?
A. Do you mean what was the content of it?
Q. No. I'm asking how do you, like -- how do you remember that that -- when you say, I've gotten feedback, that it was one e-mail from Lukas Vrbecky?
A. I've seen the copy of the e-mail that was sent.
Q. And did anyone else besides Lukas Vrbecky give you feedback that you don't do some of the things in the statement below?
A. No.

Q. And sitting here today, how do you know that he's the only one that gave you that feedback?
A. This e-mail is in direct response to exactly what he gave me as a response in his e-mail. The quote, We don't do some of the things, is exactly the feedback that he gave me.
Q. And so you didn't receive any feedback from anyone else in response to your earlier e-mail?
MR. TURNER: Asked and answered. Go ahead.
A. I did not. And, in fact, in his response where he gives me the feedback that he's gotten feedback, we don't, he clarifies that it isn't that we don't do them, it's a lack of awareness.
BY MR. CARNEY:
Q. The feedback that you don't do some of the things indicated in the statement below, what things was it that you didn't do?
MR. TURNER: Object to form.
A. Again, the feedback literally was, We don't do some of those things. There was no list. I don't know who gave the feedback to Lukas. There was no indication of what we did or didn't do in that feedback, and I knew that we did those things.

BY MR. CARNEY:
Q. And then in the next sentence you say: I want to make sure that you all have an answer to this.
Why was it important that all of the engineering managers have an answer to this if only one engineering manager was getting that feedback?
A. In the spirit of awareness, generally, I knew that we were doing those things. Lukas Vrbecky who gave me this knew that we were doing these things and I knew that the SDL would bring the awareness we were looking for. It was also 5:00 in the afternoon. I'm addressing a very large organization. It was a quick e-mail to say, Hey, you don't need to worry about these things. We are doing these things. The SDL will help consolidate these activities, formalize and standardize these activities.
Q. The concerns or issues that Lukas Vrbecky raised with you, did you report them up to anyone else above you?
MR. TURNER: Objection to form.
A. In my response, you can see the list of -- distribution list is the exact same management level that received the original e-mail.

BY MR. CARNEY:
Q. And I want -- are any of the people that you're sending it to people that you report to that are above you?
A. Yes.
Q. And who would that include?
A. Joe Kim.
Q. Which distribution group do you understand Joe Kim to be in?
A. CTO direct reports.
Q. Anyone else above you that this would have gone to?
A. And to clarify, Joe Kim would have been a member of CTO direct reports, Austin engineering and several others. There were other senior leaders I did not report to that were -- received this e-mail.
Q. Did you report to Joe Kim?
A. I reported directly to Joe Kim.
Q. In this time frame you did?
A. Yes.
Q. Had Joe Kim tasked you with developing the SDL process that we've been talking about today?
A. No. Lee McClendon tasked me with liaisoning between engineering and the GDPR consultant. That's what initiated this.

Q. Did Joe Kim have any role in directing your activities with respect to the SDL?
A. I don't remember my interactions with Joe Kim from six years ago.
Q. But in -- that's fair. I'm talking on a big-picture level, did he have any involvement in you putting together this SDL process that you've been describing?
MR. TURNER: Object to form.
A. When you say "putting together," what do you mean?
BY MR. CARNEY:
Q. So, for instance, you put together a PowerPoint presentation and training for engineers. Did Joe Kim ask you to do that?
A. No, he did not.
Q. And you talked about gather -- going around gathering documentation to assist in compiling the SDL process. Did Joe Kim have any involvement in asking you to do that?
A. No, that was initiated with Lee McClendon.
Q. All right. In your response -- where you say: I want to make sure you have an answer to this. In the next paragraph you say: The simple

response is there is improvement needed to be able to meet the security expectations of a secure development lifecycle.

What did you mean that there was improvement needed to be able to meet the expectations of a secure development lifecycle?

A. I am referring to the SDL title process that I was rolling out and the expectations that it had in adding some process improvements to our release checklist, the final security review and bringing those artifacts together for the final security review.

Q. So what were the security expectations that you're referring to in that sentence there?

A. The expectation that engineers produce the required documentation for a final security review, that the product owners responsible for the release checklist process were meeting the milestones in the checklist before we could release.

Q. And sitting here today six and a half years later, how do you know that the improvements you're talking about here are confined to the checklist?

MR. TURNER: Objection to form.

A. I don't understand what you mean by

"confined to the checklist."

BY MR. CARNEY:

Q. So it sounds like you were saying that the security expectations you're referring to here are this FSR checklist that you had implemented; is that right?

A. Yes.

Q. And how do you know that the improvement to security expectations that you're referring to here relates to the FSR checklist?

A. We produced an artifact from -- we started to produce an FSR artifact that indicated the security posture of the product that was assessed before we released.

Q. I guess I'm wondering, you don't mention the FSR checklist in this e-mail, do you?

A. This is a very generic response to a very large organization, the bulk of which are remote from me, at 5:00 in the afternoon after a long day of sending e-mails. I didn't put a tremendous amount of thought into constructing this other than to say, Don't worry, we're doing these things, it's fine, the SDL will bring visibility to what -- the good work you guys are doing currently.

Q. Okay. And understanding it was an e-mail

you quickly sent out six and a half years ago, how do you know that the e-mail related to the FSR checklist?

MR. TURNER: Objection to form.

A. I don't understand that question.

BY MR. CARNEY:

Q. Well, let me ask. Could the security -- it says there's improvement needed to be able to meet the security expectations of a secure development lifecycle.

Could there be improvement that was needed in -- with respect to other security expectations beyond the FSR checklist?

MR. TURNER: Object to form.

A. That's a very broad question. Can anyone improve at any time in -- if you're referring to does this indicate that we needed to start doing things? The answer's no, we have been doing those things. The things indicated in the security statement that are separate from the SDL, capitalized, those things we were doing at this time.

BY MR. CARNEY:

Q. So if we look at the text that you copied below from the security statement software

development lifecycle, where does it talk about the final security review checklist?

A. It does not.

Q. And so I guess what I'm asking is why do you believe now that the response to that we're not doing some of the things indicated in the statement below --

A. I don't.

Q. Okay. So let me finish my question. I'm sorry.

A. Sorry.

Q. So you say in the e-mail in response to the feedback that you're not doing some of the things in the statement below that you want to make sure that they have an answer, and your answer is there is improvement needed to be able to meet the security expectations of a secure development lifecycle.

And I'm wondering, since the software development lifecycle statement below says nothing about the final security review checklist, why do you think that's what you were talking about?

A. Because that's the scope of which I was focused on at the time was bringing this process together that introduced a new process called the

the bottom of the e-mail because you made reference now to the -- that portion of the security statement that you believed the company was doing those things already. So I want to ask you some questions about that.

In the first sentence of the second paragraph it states: Our secure development lifecycle follows standard security practices including vulnerability testing, regression testing, penetration testing and product security assessments.

In the context of the security statement here, do you understand what is vulnerability testing?

A. I do.

Q. And what is that?

A. Vulnerability testing is continuing testing activity where you are ensuring that the security controls you have implemented in the product are, in fact, functioning the way they should.

Q. And at this time in 2018, was SolarWinds using vulnerability testing in the development of all its software products?

A. I can speak to the products that I was

responsible for and that security testing was one of the milestones in -- that was required in our release checklist.

Q. And specifically vulnerability testing?

A. Yes.

Q. And was -- do you know whether vulnerability testing was used at that point in time for developing software associated with Orion?

A. Yes.

Q. And was it?

A. Yes, it was.

Q. And how about regression testing as it's used in the security statement, do you understand what that's referring to?

A. Yes, I do.

Q. And what is regression testing?

A. It's ensuring that the new code you have implemented has not disrupted the existing code in any negative degradation, no degradation in functionality or security.

Q. And with respect to the products that you're familiar with, at this point in time in 2018, was SolarWinds using regression testing in development of all its software products?

A. Absolutely.

Q. And how do you know that?

A. It's part of the release checklist. It's standard software development. You cannot release without testing the code you've implemented and make sure it works correctly.

Q. And was this regression testing done in conjunction with the Orion product, to your awareness?

A. Yes.

Q. And how do you know that?

A. It's standard process. It's just software development.

Q. And it also uses the term "penetration testing" here. Do you understand what it means in the context of the security statement?

A. I do.

Q. And what is penetration testing?

A. Very, very closely related to vulnerability testing. You're ensuring the security controls that you've implemented are working correctly by specifically testing aspects of the product periodically.

Q. And with respect to the products you were familiar with, at this time was SolarWinds using penetration testing for all its products?

A. We had an internal security testing that was responsible for scheduling and working with the teams to plan for those and execute those penetration tests.

Q. And what organization was that internal security testing team part of?

A. It was within -- it was within engineering.

Q. And did they report to you?

A. They did not report to me.

Q. And was penetration testing being used on the Orion product at that time?

A. Yes.

Q. And how do you know that?

A. I recall communications planning for scheduling certain aspects of the product to go through penetration testing, or pen testing for short.

Q. In what time frame?

A. This time frame to current.

Q. And next it talks about product security assessments.

Are you familiar with how that term is being used in the security statement?

A. Yes.

teams and multiple spaces within the engineering Confluence platform including personal spaces. There's a tremendous amount of documentation.

Q. And was one of the goals of your SDL project to take all that widespread documentation and pull it together in one document that you could show someone?

A. Referring back to the catalyst for this project, pulling this documentation security-related for the GDPR consultant was -- one of the goals was to consolidate this into something that was consumable and understandable by...

Q. All right. Sir, if I could now turn your attention to Exhibit 6. This is a e-mail string. The e-mails on the bottom from May 2018, at the top from September 2018. And it starts with the Bates stamp SW-SEC00237608.

Are you familiar with this document?

A. I don't recall it from the time frame, but I see that my response is here.

Q. And the e-mails to which you are carbon copied on, would you have received those in the course of your work at SolarWinds?

A. Yes.

Q. And the -- referring to the middle

e-mail, that's an e-mail that you sent on May 21st, 2018; is that correct?

A. May 1st [sic], 2018, yes.

Q. You say in the -- in your e-mail: I don't see a line item about threat modeling, but since you mentioned it.

What did you mean by that?

A. Reviewing this, I see the phrase: Please confirm particularly the threat modeling, but I see no reference to this anywhere else so I was unclear why they were mentioning it at the time.

Q. And just so we're clear for the record, because the e-mail at the bottom that lists all the different security capabilities, you don't see anything that covers threat modeling down there?

A. There's nothing listed here.

Q. In the next paragraph you say: TM'ing is a process.

First of all, is TM'ing threat modeling?

A. Yes.

Q. And what did you mean that threat modeling is a process?

A. In a very general sense how you approach threat modeling is a process you can apply to your software development activities.

Q. And in the next sentence, and I'll -- it says it's part of the SDL.

What did you mean that threat modeling is part of the SDL?

A. It's an area of improvement that I wanted to focus on. Currently the artifacts that were coming from the threat modeling that we were doing were not well documented as I've referred to before. And part of my project was to improve the artifacts that were coming from those activities in a more formal, formal manner. That was an additional thing that's not part of our security statement.

Q. What do you mean it's not part of your security statement?

A. Again, when I go back to our security statement that was public-facing, we're focused on vulnerability testing, regression testing, pen testing, product security awareness -- or assessments, sorry. While we were doing threat modeling internally, it's an inherent part of the software development activities, as we talked about previously when you assess risk and mitigate that risk. I felt we could formalize that process and improve that process.

Q. And I think you said it's an area of --

where improvement was needed.

What kind of improvement was needed with respect to threat modeling?

MR. TURNER: Objection, asked and answered.

A. Again, I can threat model and I can implement the outputs of that threat model without necessarily documenting what I did and be effective in my security controls. I wanted to formalize that process and produce artifacts to improve efficiency.

BY MR. CARNEY:

Q. Correct me if I'm wrong, but did you say earlier that threat modeling is a part of product security assessment?

A. I don't believe I made that comment.

Q. Is threat modeling a part of product security assessment?

A. Depends on what you're talking about when you use the term "product security assessment."

Q. Okay. So if we look back at Exhibit 5 where it has the software development lifecycle description at the bottom of the e-mail.

Do you see that?

A. I do.

Q. And it says: Our secure development

lifecycle follows standard security practices including vulnerability testing, regression testing, penetration testing and product security assessments.

I'm wondering, in that context is threat modeling incorporated into product security assessments?

A. I did not write this statement. I didn't participate in writing this statement, so I can't be definitive in terms of what the scope of product security assessments might mean. I can interpret what I felt they -- that it meant.

Q. And do you interpret it to include threat modeling?

A. I interpret this to assess the outputs of the previous activities that are listed there.

Q. And just looking at that entire description there of software development lifecycle, is there any part of that two-paragraph description that you think incorporates threat modeling?

A. You could potentially put threat modeling anywhere. It's just an additional activity that you may choose to do informally or formally, but inherently it just happens as part of the software development process.

Q. In the next part of the sentence in Exhibit 6 you say -- referring to threat modeling, you say: It's part of the SDL and we are just barely beginning to understand how teams are going to be doing this activity.

What did you mean by that?

A. I wanted to improve the process. I was trying to determine what options we had in terms of producing that documentation and tracking that documentation that I had not yet settled on.

Q. But what does it mean that you were barely beginning to understand how teams are going to be doing this activity, the threat modeling?

A. In this case, we're talking about six years ago, it's just phrasing.

Q. Okay. So you don't think you were talking about doing the threat modeling itself here?

A. Threat modeling, no. It was already happening.

Q. So if you look at the bottom e-mail from Rani Johnson where she's listing in the left column security capabilities and in the right column the tools, what did you understand this to be describing?

A. Are you asking about the complete table

or are you asking about what the columns mean?

Q. Yeah, just the complete table. What did you understand her to be trying to convey through this table, just as a whole?

A. I was not involved in putting this table together. I believe that I was associated with this e-mail because we list some of the tools that engineering was using for some of these security activities.

Q. And which of the security activities in the table would you have given input on?

A. I don't recall giving input on any of these, but I would have been -- what would have been relative to me would have been code analysis and pen testing.

Q. So just using pen testing as an example, the -- pen testing is in the left column and then in the right column -- so, for instance, Rapid7, Metasploit, is that a pen testing tool?

A. That is one of various pen testing tools that we were using.

Q. So the -- is it fair to say the right column describes the tools that were being used for pen testing?

A. That's my understanding.

Q. And in your e-mail, though, when you say: We're barely beginning to understand how teams are going to be doing this activity, you don't think you were referring to how the teams were actually going to be performing threat modeling and what tools they were going to use?

A. I was referring to the improvement in that process that I was trying to assess and take action on.

Q. Okay. And I guess what I'm trying to understand is that Rani Johnson is creating this table that shows the different security capabilities and the tools that are used to achieve those.

Do you think that you are telling her, We don't know what tools we're going to use for threat modeling?

A. I was implying that I wanted to improve the process, that I was evaluating various methods for doing -- for improving the TM'ing process, the threat modeling process, and I had yet to understand the best way that would be applicable for out teams to improve that.

Q. And evaluating various methods for improving the threat modeling process, would that be evaluating different tools that you could use for

threat modeling?
A. Different tools and different processes within the broad process of threat modeling. Threat modeling can be done verbally, it can be done on a piece of paper, it can be done on a whiteboard or you can use a formal tool to produce that documentation. There's multiple ways to do this exercise.
Q. Do you recall if at any point after this you responded to her and said, Here's your answer now, these are the tools we use for threat modeling?
A. Not that I'm aware of.
Q. And I'll just note for the record that -- and you're not copied on this, but at the top she's reforwarding this e-mail in September of 2018.
Do you have an understanding of why she would have been forwarding your e-mail in September of 2018?
A. I have no idea.
Q. By September of 2018, had you -- putting aside what you might have told Ms. Johnson about it, had you kind of figured out the answer what tools you were going to use for threat modeling?
A. I believe we continued to use the same internal process that we were doing.

Q. Did you ever come to understand why Ms. Johnson was asking you to confirm particularly with respect to threat modeling?
A. I don't know. And you can -- from this e-mail, there is no reference other than the subject line, so I don't have an understanding. I wasn't involved in compiling any of this data.
Q. Fair enough. But you don't recall having a subsequent oral conversation with Ms. Johnson about --
A. No.
Q. -- this issue?
A. I don't remember anything, no.
Q. Is she someone that you work with on a regular basis?
A. I wouldn't say a regular basis, no.
Q. Were you both in the same office?
A. No.
Q. Which office are you in?
A. I was remote in Utah and she was in the Austin office.
Q. Are you still remote now?
A. Yes.
Q. And where in Utah?
A. I live in Eden, Utah.

Q. So you work from home, is that --
A. Yes.
(Deposition Exhibit 7 marked for identification.)
BY MR. CARNEY:
Q. All right. Mr. Colquitt, again, take as much time as you need to look over the document, but just for the record, I've handed you what's been marked as Exhibit 7. It's a May 1st, 2018, e-mail, subject, Monthly technology newsletter for April 2018, and it begins at Bates stamp SW-SEC00016513.
Mr. Colquitt, did you have sort of regular involvement in putting together the monthly technology newsletters?
A. I contributed a few times to the newsletter.
Q. And just as -- I'm not asking you about the specific one yet, but just as a general matter, how would you go about contributing to the monthly technology newsletter? So for instance, who would ask you to do it and how would it come about?
A. I don't remember specifics of how it came about. We would receive an assignment to -- it's your turn to produce some area of the newsletter,

different people would contribute. So we would write our piece and contribute. I think it would be compiled by Paul Gray?
Q. And who is Paul Gray?
A. He was head of architecture.
Q. And you said that you would receive an assignment. Who would you receive an assignment from?
A. I would have -- it would have been asked either by Joe or by Paul.
Q. So either by Joe Kim or by Paul Gray?
A. Yes.
Q. And, sir, if I could ask you to turn to the fourth page of this -- let's see. Let me get you on the right page.
So if you look at the page that at the bottom, the last numbers are 16519, the bottom right corner.
A. Uh-huh.
Q. And there's a blue little header that says SolarWinds Security Series. And if you flip over to the next page, it says Steven Colquitt, director software engineering SolarWinds.
A. Uh-huh.
Q. Would you have put together this section

that take?
A. Within our products, there are security controls to protect and secure that piece of software. Those are the security activities that happen during development.
Q. Would you include threat modeling in the category of security and security testing that are implemented throughout the entire software development methodology?
A. I would say that as an inherent aspect of implementing a mitigation to a security risk is inherently a threat modeling.
Q. What do you mean by "implementing a mitigation to a security risk"?
A. As an engineer when you are implementing a piece of functionality, you will assess the user or data interaction in that piece of functionality and you will assess whether there's a risk there. And if there is, you will put in a mitigation. For example, you may choose to encrypt that piece of data as it is transiting between trust boundaries.
(Deposition Exhibit 9 marked for identification.)
BY MR. CARNEY:
Q. And, Mr. Colquitt, I've handed you -- I

didn't actually hand it to you, but you've been handed what's been marked as Exhibit 9. And this is a PowerPoint presentation that begins at SW-SEC00262250. And you, once again, take as much time as you need. I'm only going to ask you right now about one page of the document. But have you ever seen this document before?
A. No, not until just now.
Q. Do you know what a KBT offsite is?
A. KBT is the initials of our previous CEO.
Q. Is that Kevin Thompson?
A. Kevin Thompson.
Q. Have you ever been to a KBT offsite?
A. That's way above my pay grade. No.
Q. Have you ever been to any CEO offsite?
A. No.
Q. Would you like to go to one?
A. Yes.
THE WITNESS: Come on, Jason. Make it happen.
BY MR. CARNEY:
Q. All right. So if I can just ask you to look at the second-to-last page of the document, sir. And understanding that this isn't a document that you've seen, so I'm just asking for your best

understanding, if any. But if you look at the second row on the chart there on the page ending in 262260 --
A. Uh-huh.
Q. -- the second row says: Description pen testing. And then in the notes it says: Unfunded in FY18, plan to pen test eight to ten products in 2019.
Do you know what it means that pen testing was unfunded in FY18?
A. So to clarify, I had no involvement in compiling this data. I don't also understand or know the criteria that would have been used to come up with this. My assumption is they were referring to external pen testing to augment the internal penetration testing that we were already doing.
Q. So if you were doing internal pen testing, would there be a cost reflected in the budget somewhere?
MR. TURNER: Objection, foundation.
You can answer if you know.
A. Internal pen testing was done by internal employees that were hired on a security team, so that budget would have been head count budget.

BY MR. CARNEY:
Q. Got it. And is that where you're deriving your understanding that unfunded means external pen testing?
A. Yes, because I know we had an internal team doing pen testing.
Q. And the internal team was doing pen testing in 2018?
A. Yes.
(Deposition Exhibit 10 marked for identification.)
BY MR. CARNEY:
Q. Mr. Colquitt, you've been handed what's been marked as Exhibit 10. It's a document entitled MSP -- it's M, as in Mike, SP Products, Security Evaluation, Confidential, July 2019, and it has the Bates stamp on the first page of SW-SEC00166790.
And once again, take as much time as you need, I'm only going to show you one part of it, but have you ever seen this document before?
A. As of the last week and a half, yes.
Q. Do you know -- before the past week and a half, had you ever seen this document before?
A. No, sir.
Q. Do you know who Stas Starikevich is?

A. No.
Q. Do you know who -- my apologies -- Wojciech Pitera is?
A. My guess would be Wojciech, but, no, I don't know who that is.
Q. And I can spell those for the -- Stas is S-t-a-s, last name S-t-a-r-i-k-e-v-i-c-h. And then the second name Wojciech is W-o-j-c-i-e-c-h, last name P-i-t-e-r-a.
Do you have any understanding of what this document is or why it exists apart from what counsel might have told you?
A. No.
Q. If I can just ask you to turn to the page ending in 166794, and the first bold item on the page is: Resilience requirements are established for critical services.
Do you see that page?
A. I do.
Q. First of all, what is MSP as it's used in the SolarWinds context?
A. MSP is an acronym for managed service provider.
Q. And what is a managed service provider?
A. It's when a company provides a service

that's hosted outside of the customer's environment that the customer can access.
Q. And is -- what is the name of SolarWinds' MSP product?
A. I was not involved with SolarWinds' MSP. I don't remember all the products. I can reference the first front page, I think where they mention some products on here, but I wasn't -- I'm not familiar with these products at all.
Q. So let me just ask you one question on understanding that background. In the middle of that page we were just looking at ending in 166794, it says -- under the heading Threats Internal and External Are Identified and Documented, it says underneath it: No threat modeling nor analysis is performed as part of any process, and then in parentheses it says: Except MSP backup engineering.
Do you have any knowledge one way or another whether that statement is true or not?
A. I don't have any idea what criteria they would have been looking at to make that assessment.
Q. Do you have -- independent of this document, do you have any knowledge as to whether threat modeling or analysis was used as part of the MSP products?

MR. TURNER: Objection to form.
A. I cannot speak to any of the MSP products or MSP engineering. I can speak to generally it's impossible to deliver security controls in a product without having done threat analysis.
BY MR. CARNEY:
Q. Is it -- is threat analysis different from threat modeling?
A. I think I just use that term -- the same thing. I'm using that interchangeably. Threat modeling and threat analysis, that's what I meant. I was referring to threat modeling.
Q. Okay. Great. So is it fair to say, then, it's impossible to deliver security controls in a product without having done threat modeling?
A. I'm saying is that threat modeling is an assessment of risk at a particular point in which you choose to mitigate with a security control. That is threat modeling. So I do not understand what criteria they're using here to make that assessment. They may be thinking of more of a formal process that they would like to achieve. I'm not sure.
Q. And putting aside that document, were MSP products part of your SDL project?

MR. TURNER: Objection to form.
A. The MS -- the SDL project, again, was a process that was overlaying our engineering activities, which would have been -- training would have been rolled out to this team as well.
BY MR. CARNEY:
Q. So that process would have been applied to MSP at some point?
A. They would have received training, yes.
(Deposition Exhibit 11 marked for identification.)
BY MR. CARNEY:
Q. Mr. Colquitt, you've been handed what's been marked as Exhibit 11. And this is a string of e-mails from March of 2018 and it begins with the Bates stamp SW-SEC00013553.
You familiar with this e-mail chain?
A. Too long ago. I don't remember this exchange.
Q. Okay. And if you notice, the initial e-mail, which starts at the bottom of page 1, it's from -- the one and the same, Wojciech Pitera from the previous document; is that right?
MR. TURNER: Can you give the witness just a chance to review it.

Q. So how, for example, would the final security review requirement help improve the outputs of those activities?
A. So each of those activities had an output that needed to be assessed. You needed to assess the quality bar produced from regression, from vulnerability, from pen testing. It brought all of those into a central formalized consistent document that could then be reviewed at each point to establish an overall security posture, how well did we do security.
Q. And could that help improve the quality of those activities?
A. Absolutely, knowing that you have to produce that documentation will improve your focus as an engineer on what you have to produce.
Q. So if we could go back to the training in Exhibit 3. Now, did this training just cover the new documentation requirements you entered -- well, let me actually ask a different way.
Let's turn to the document -- the page ending in Bates stamp 85. And do you see any reference there to the new documentation requirements you introduced?
A. Yes, final security review and review

collateral.
Q. Okay. So fair to say that the training did cover those new documentation requirements?
A. Yes.
Q. But as I think the SEC pointed out in its questioning, the training wasn't just about that, right, it covered other issues as well; is that right?
A. It focused on additional outputs and collateral of the activities that were in place and brought them together into a formalized consistent process.
Q. Well, let's look beyond this page, though, and look at the page marked ending with the Bates stamp 78. This is the diagram of all the components of the SDL at SolarWinds, right?
A. Yes.
Q. And your training went through each of those elements in the following pages, right?
A. Yes.
Q. So what was the purpose of going through, you know, the entire SDL like that as part of this training?
A. Each of those phases is quite broad and can be applied in different ways. And so training

teams on all the different aspects of the phases and what -- what needed to be produced was a goal of that.
Q. Let me put it a different way. Who was this training directed to?
A. This training was directed to entire engineering teams and their leadership teams. Regardless of seniority level or what your role was every single engineer received this training.
Q. So this is the entire engineering staff at SolarWinds?
A. Yes.
MR. CARNEY: Objection, form.
BY MR. TURNER:
Q. So would that include just the engineers who would have involvement in security or would there be other engineers who wouldn't have that involvement?
MR. CARNEY: Objection, vague.
A. This trained -- if you're an engineer committing code or testing code or contributing to the production of a piece of software that would be sold to customers, you were trained on the security lifecycle.

BY MR. TURNER:
Q. Great. So again, my question is would that include just engineers who would have involvement in security activities or would there be a broader set of engineers?
A. All engineers, whether they were involved in security activities or not.
Q. Can you give me an example of, like, who's an engineer who would not be involved in security?
A. Yeah. A great example would be an associate-level engineer who might be given a very limited scope of work to complete because of lack of experience would probably not be involved in assessing a particular security risk as part of the entire workflow. That would be left to senior -- more senior, more experienced engineers.
Q. I think you mentioned that when you first started at -- as a young software engineer, what was the company again?
A. Altiris.
Q. What was your position there?
A. I was a UI developer.
Q. What's UI?
A. User interface developer.

Q. Is that all you worked on?
A. At the beginning, yes, very limited scope of work.
Q. Are there similar engineers at SolarWinds who work on --
A. Yes, absolutely.
Q. Would those engineers do penetration testing, for example?
A. They would not directly be involved in penetration testing.
Q. Or vulnerability testing?
A. They wouldn't be directly involved in that.
Q. So is it fair to say -- would all of the attendees of this training you did, would they have had a preexisting familiarity with the concepts you went over, or would the concepts potentially be new to some of the attendees?
MR. CARNEY: Objection, calls for speculation.
BY MR. TURNER:
Q. Does that require speculation or do you know?
A. No, and the industry's an evolving industry all the time and new terms evolve all the

time. When you use terms such as "penetration testing," as a new engineer I had no idea what that was. It wasn't until I was a more senior. So, yes, there's a lot of terminology that's used very broadly across the industry that would be very confusing on top of the fact that many of these guys aren't native English speakers. So terminology was very -- probably a very confusing aspect.
Q. Okay. But I'm just -- I'm going back to -- you testified just a minute ago that some of the engineers attending this training would not have had prior involvement in security aspects of the development lifecycle.
A. Yes.
Q. Is that fair?
A. That is fair.
Q. So would you expect the concepts you're going over in this document potentially to be new to those individuals as opposed to engineers who had, you know, prior involvement with security aspects of code development?
A. Yes, that is a true statement.
Q. So what was the purpose of providing this training to all attendees? Why did you -- why were you giving this training to engineers who might not

have a security role?
A. As a company creating a broader awareness of our approach to security just improves the overall process. It improves our overall approach, and it improves the quality of the outputs. So training everyone to be involved in security regardless of their role was an important aspect of the SDL training.
Q. And I think you testified earlier about wanting to increase I think you said exposure or visibility for the SDL.
How, if at all, did this training relate to that?
A. Training broadly across the engineering teams introduced a formality and a consistency in our approach that some of those engineers might not have been familiar with prior, so this training brought that level of awareness to each of those individuals -- those roles, those differing roles.
Q. Now, was this training designed to actually, like, teach engineers how to do penetration testing?
A. No.
Q. Or how to do regression testing?
A. No.

Q. Why not?
A. Those things were already happening. Those things are part of our methodology, our approach to software. That's just software development.
Q. Could you teach those things in, like, a, you know, 30-minute or hour-long training?
A. No.
Q. So that wasn't the goal of this training?
A. No.
MR. CARNEY: Objection, vague.
BY MR. TURNER:
Q. You were asked earlier about this e-mail that you sent out on January 30th. It's Exhibit 4. So you said in this -- in the top line of this e-mail: Managers, I've gotten feedback that we don't do some of the things that are indicated in the statement below.
Do you see that?
A. Yes, I do.
Q. And I think you testified earlier that the feedback you were referring to had come from Lukas Vrbecky?
A. Correct.
Q. Let me show you what we'll mark as --

MR. TURNER: What, Exhibit D-1? Or how do you want to do it?
MR. CARNEY: 13.
MR. TURNER: Just go sequentially? That's fine. Let's mark it as 13.
THE WITNESS: Do I need to give that to you?
(Deposition Exhibit 13 marked for identification.)
BY MR. TURNER:
Q. So on Exhibit 13, this is an e-mail to you from Lukas Vrbecky, right?
A. Yes.
Q. And it's sent about four hours or so before you sent your e-mail reflected in Exhibit 4?
A. Okay. Yes.
Q. Is that correct?
A. Yes.
Q. So is this the e-mail you were referring to earlier?
A. This is the e-mail I was referring to earlier.
Q. Let's start with the e-mail at the bottom of the chain. So this is the e-mail that you are sending out to all engineering managers, right?

A. Correct.
Q. With the excerpt from the security statement?
A. Yes.
Q. And your e-mail sending that excerpt out is sent to I think you testified earlier all engineering managers?
A. Yes.
Q. And you had suggested in the e-mail to these managers: Please share with your teams. Right?
A. Yes.
Q. What did that mean? Who did you expect them to share this with?
A. So each of those managers would have had responsibility or direct reports, multiple direct reports and multiple teams reporting in to them, and the intention was for them to disseminate that information down through their team.
Q. So would that encompass, again, all engineering staff at the company?
A. All engineering staff regardless of role, regardless of seniority.
Q. So again, that would include some people who didn't have a security role --

A. Yes.
Q. -- previously at the company?
A. Yes. Yes, correct.
Q. He e-mails you back in the following e-mail on January 29th saying: Steven, this is a great progress in formalizing our security process.
What did you understand him to have meant by formalizing?
A. Lukas recognized that we were already doing the underlying activities, but by compiling a concise formalized statement, that made it more clear what our approach to security was, was what he was referencing when he says formalizing the process.
Q. And what awareness did Lukas have, if any, of the SDL project you were working on at the time?
A. Lukas had been helping me with certain aspects. I think he also had responsibility for some of the security team activities in his role.
Q. Okay. And then you say -- sorry, before we go there. He asked you whether you could share more information about, quote, The high-level plan on how we are improving software development lifecycle in the upcoming months.

Do you see that in his e-mail?
A. Uh-huh.
Q. And then you respond: Hey, Lukas, I am now in the process of -- is hosting SDL training. And then you detail the various places you're going to go in your training.
A. Uh-huh.
Q. And then he says: I think that would be great. It came back from teams as a feedback that we actually don't do things and actions that are in the statement.
That's the line you quoted in your --
A. Yes.
Q. -- subsequent e-mail, right?
A. Uh-huh.
MR. CARNEY: Objection, characterization.
BY MR. TURNER:
Q. But then he adds: I'd say more accurate would be that teams are not fully aware about the scope of what we do and also what we are going to do by the end of Q1.
What did you understand him to mean by that?
A. So he understood that there were

engineers on teams who probably weren't involved in aspects of things like pen testing, vulnerability testing, who didn't have direct knowledge that those activities were happening and he was aware that we were improving the process by implementing things like the final security review they weren't aware of yet because I hadn't rolled out training.

Q. Okay. And then you say: For these kinds of questions coming from team, I would like managers to have a canned answer, smiley face.

Is that what leads you to send your e-mail a few hours later?

A. Yes.

Q. And you say -- the simple response is: There is improvement needed to be able to meet the security expectations of a secure development lifecycle.

Now, were you referring to the improvements you were making as part of your SDL project?

A. I was.

MR. CARNEY: Objection, leading.

BY MR. TURNER:

Q. And what type of improvements, again, was your SDL project focused on making?

A. Again, mainly it brought awareness; two, it formalized the outputs, formalized documentation; and, third, it introduced some additional process that would facilitate bringing that documentation together.

Q. And you talk about needing -- excuse me, improvement needed to meet the security expectations of a secure development lifecycle.

What new expectations was SolarWinds expected to meet around this time?

MR. CARNEY: Objection, form.

A. So, one, we were -- we focused on GDPR compliance where we were expected to be -- to produce demonstrable evidence of our security practices and, two, more and more customers were beginning to put a focus on security and were asking for evidence.

BY MR. TURNER:

Q. Can we take a look at the security statement. Exhibit 10.

MR. LUONGO: That wasn't an exhibit to this deposition.

MR. TURNER: Sorry.

BY MR. TURNER:

Q. Actually we can stick on Exhibit 4 and

just use the quote at the bottom of that first page. The first sentence -- I just want to be clear for the record, that first sentence says: We follow a defined methodology for developing secure software that is designed to increase the resiliency and trustworthiness of our products.

Was that true while you were at SolarWinds?

A. That was true.

MR. CARNEY: Objection, foundation.

BY MR. CARNEY:

Q. And the methodology that was followed for the software development lifecycle, I think before you testified that was Agile; is that right?

A. Yes.

Q. And is that a defined methodology as far as you understand it?

A. It is an industry standard framework that's adopted per the needs of a particular software company and then defined internally for that software team.

Q. So is it defined in the industry?

A. Yes.

Q. And it's defined at SolarWinds?

A. Internally, yes.

Q. How would it have been defined internally?

A. We would have had documentation on how we do software at SolarWinds.

Q. Where would that base have been maintained?

A. In the engineering space of Confluence.

Q. First sentence of the second paragraph: Our secure development lifecycle follows standard security practices including vulnerability testing, regression testing, penetration testing, and product security assessments.

Just to make sure we're clear for the record, were all those things done at SolarWinds?

A. Yes.

MR. CARNEY: Objection, foundation.

BY MR. CARNEY:

Q. Let me finish my question first. Was that statement true at the time of the -- this e-mail?

MR. CARNEY: Objection, foundation.

BY MR. CARNEY:

Q. Was that statement true?

A. Yes, it was true.

Q. And how do you know?

A. Outputs, documentation and I was also participating in the release checklist.
Q. And when you say outputs and documentation, was this around the same time when you were looking for those artifacts as part of your GDPR compliance work?
A. This would have been --
MR. CARNEY: Objection, vague.
BY MR. CARNEY:
Q. Just let him finish to make sure you guys don't talk over each other.
So did you understand my question?
A. No.
Q. When you say outputs and documentation, was this e-mail written around the same time when you were looking for artifacts -- scratch that. Let me ask a different way.
As part of your SDL project, I believe you mentioned earlier you had looked for documentation and artifacts of security practices in the development lifecycle; is that right?
A. Yes.
Q. And where did you look for those artifacts?
A. In Confluence.

Q. And so as part of that work, did you see evidence of these practices that are listed here by teams other than your own?
A. Yes, I did.
Q. You were asked several times about threat modeling. And I just want to try to cut through the jargon a little bit and see if I can get an understanding of what that term means at a very basic level.
Can you give me one?
A. Yes. It's when you assess the risk that there might be an opportunity for someone to sort of get around the security that you've implemented in your product.
Q. And I think you testified at one point that it's impossible to have security controls if you don't have threat modeling. And I just want to make sure I have the logical structure of that statement right.
What did you mean by that?
A. I mean that our products had security controls in them. Those security controls are the outputs of a threat model having taken place.
Q. So in other words, if there are security controls as part of a product, does that necessarily

imply that threat modeling has been done?
A. Yes, it does.
MR. CARNEY: Objection, leading.
MR. TURNER: Okay. No further questions.
MR. CARNEY: Thanks. Very, very briefly.
FURTHER EXAMINATION
BY MR. CARNEY:
Q. Mr. Colquitt, if I could ask you to look at Exhibit 13 that Mr. Turner just showed you. And if you look at the top, it's the e-mail from Lukas Vrbecky to you; is that right?
A. Yes.
Q. And he says in the second sentence: It came back from teams as a feedback that we actually don't do things and actions that are in the statement.
And you said that's what you were referring to in your -- your e-mail that's reflected in Exhibit 4?
A. Yes.
Q. And then he says in the next sentence that -- of Exhibit 13: I'd say more accurate would be that teams are not fully aware about the scope of

what we do and also what we're going to do by the end of quarter 1, right?
A. That's what he says here.
Q. Okay. And if we look back at Exhibit 4, in your response to the managers when you're giving them an answer, you didn't say, We're doing all these things already, did you?
A. That's not in my response.
Q. And you didn't see to -- say to them that the teams are just not fully aware of the scope of what we're doing.
Did you say that?
A. I did not say that.
Q. Okay. You did say there is improvement needed to be able to meet the security expectations of a secure development lifecycle, right?
A. Yes.
MR. CARNEY: I have no further questions.
FURTHER EXAMINATION
BY MR. TURNER:
Q. Mr. Colquitt, when you wrote this e-mail, did you imagine that a swarm of SEC lawyers was going to be poring over every word you wrote seven years later -- or six years later?

THE VIDEOGRAPHER: This concludes today's testimony of Steven Colquitt. Going off the record. Time is 4:56.

(Deposition concluded at 4:56 p.m.)

REPORTER'S CERTIFICATION

I, Micheal A. Johnson, Registered Diplomate Reporter and Notary Public in and for the State of Texas, certify that on the 18th day of September, 2024 I reported the Videotaped Deposition of STEVEN COLQUITT, after the witness had first been duly cautioned and sworn to testify under oath; said deposition was subsequently transcribed by me and under my supervision and contains a full, true and complete transcription of the proceedings had at said time and place; and that reading and signing was not requested.

I further certify that I am neither counsel for nor related to any party in this cause and am not financially interested in its outcome.

GIVEN UNDER MY HAND AND SEAL of office on this 23rd day of September, 2024.

_____

MICHEAL A. JOHNSON, RDR, CRR
NCRA Registered Diplomate Reporter
NCRA Certified Realtime Reporter

Notary Public in and for the
State of Texas
My Commission Expires: 8/8/2028